BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 50 195.5

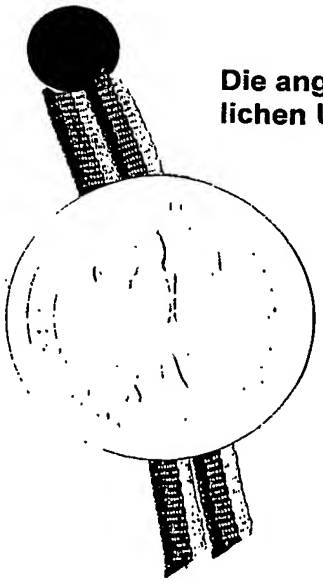
Anmeldetag: 28. Oktober 2002

Anmelder/Inhaber: Océ Printing Systems GmbH, Poing/DE

Bezeichnung: Verfahren und Anordnung zum Authentifizieren einer Bedieneinheit sowie Übertragen einer Authentifizierungsinformation zu der Bedieneinheit

IPC: H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.



München, den 5. November 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Kahle

A 9161
02/00
EDV-L

Verfahren und Anordnung zum Authentifizieren einer Bedieneinheit sowie Übertragen einer Authentifizierungsinformation zu der Bedieneinheit

Die Erfindung betrifft ein Verfahren und eine Anordnung zum Erzeugen von Authentifizierungsinformationen durch die eine Datenverarbeitungsanlage eine Authentifizierung einer Bedieneinheit durchführt. Ferner betrifft die Erfindung ein Verfahren und eine Anordnung zur Authentifizierung einer Bedieneinheit eines elektrofotografischen Drucker- oder Kopiersystems.

Bekannte elektrofotografische Drucker und Kopierer haben Kommunikationsschnittstellen, über die Bedieneinheiten und Wartungscomputer mit dem Drucker oder Kopierer zum Bedienen, zur Diagnose und zur Wartung verbunden werden können. Insbesondere mit Hilfe der Wartungscomputer können sicherheitsrelevante Einstellwerte des Druckers oder Kopierers geändert werden. Werden solche Änderungen von nicht ausreichend qualifizierten Bedienpersonen oder z.B. über eine Netzwerkverbindung, durch Unberechtigte durchgeführt, kann eine erhebliche Qualitätsverschlechterung und eine Schädigung bzw. Zerstörung von Baugruppen des Druckers oder Kopierers erfolgen.

Bei bekannten Druckern und Kopierern sind mehrere sogenannte Benutzerstufen vorgesehen, wobei eine Bedienperson eine Benutzerstufe auswählen kann und seine Berechtigung zur Auswahl dieser Benutzerstufe durch eine Passworteingabe bestätigt. Ferner besteht bei bekannten Druckern und Kopierern durch ungesicherte Zugriffe die Möglichkeit, dass unberechtigte Personen Informationen über den Aufbau und die Steuerungsstruktur des Druckers oder Kopierers mit Hilfe der Kommunikationsschnittstelle des Druckers oder Kopierers erhalten. Auch Systemparameter, wie Zählerstände des Druckers oder Kopierers, die gegebenenfalls auch für Abrechnungszwecke genutzt werden, können über die Kommunikationsschnittstelle bekannter Drucker oder Kopierer manipuliert werden.

Aus dem Europäischen Patent EP 0 513 549 A2 ist eine Anordnung zum Steuern und zum Übertragen von Daten zwischen einem Host-Computer und einer Kopierersteuerung bekannt, wobei die Kommunikation erst bei erfolgter Identifizierung des Host-Computers mit Hilfe eines Passwortes erfolgt ist. Ferner ist eine Steuereinheit zur Kommunikationssteuerung vorgesehen.

Aus dem Patent US 5,077,795 ist ein elektronisches Drucksystem bekannt, bei dem mit Hilfe eines Benutzerprofils für jeden Benutzer die Sicherheit von Nutzerdaten und Nutzerprogrammen sichergestellt ist. Die Benutzerprofile werden von einem Sicherheits-Administrator vor Ort oder von einem entfernten Ort aus verwaltet.

Jedoch bieten die bekannten Zugriffsverfahren nur einen unzureichenden Schutz von druckerinternen Daten und Einstellwerten. Insbesondere besteht bei Passwörtern ein erhebliches Sicherheitsrisiko darin, dass Passwörter mit Hilfe von Programmmodulen ausgespäht werden können, die Tastatureingaben mitschneiden. Ferner besteht ein Sicherheitsrisiko bei Passwörtern darin, dass die Passwörter dem jeweiligen Benutzer zugestellt werden müssen, wobei oft nicht sichergestellt werden kann, dass Unberechtigte Kenntnis der Passwörter bei der Übertragung und/oder Zustellung der Passwörter erhalten. Auch ist bei Passwörtern nicht sichergestellt, dass berechtigte Personen die Passwörter nicht an unberechtigte Personen weitergeben. Ein wirksamer lokaler Schutz bekannter Drucker oder Kopierer konnte nur durch das Verhindern eines physikalischen Zugriffs von unberechtigten Personen auf die Kommunikationsschnittstelle des Druckers oder Kopierers erfolgen. Jedoch ist dann auch erforderlich, dass die Druckdaten nicht über ein Netzwerk zum Drucker übertragen werden, das auch mit globalen Netzwerken, wie dem Internet, verbunden ist, über das auch unbefugte Personen Zugriff auf den Drucker erhalten. Diese Maßnahmen verhindern jedoch auch, dass eine Fernwartung, Ferndiagnose oder Fernbedienung des Druckers

durch Servicespezialisten durchgeführt werden kann, die nicht vor Ort am Drucker sind.

Aufgabe der Erfindung ist es, ein Verfahren und eine Anordnung anzugeben, durch die eine einfache Authentifizierung einer Datenverarbeitungsanlage möglich ist.

Die Aufgabe wird für ein Verfahren zur Authentifizierung einer Datenverarbeitungsanlage mit den Merkmalen des Patentanspruchs 1 gelöst. Vorteilhafte Weiterbildungen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Durch ein Verfahren zur Authentifizierung einer Datenverarbeitungsanlage mit den Merkmalen des Patentanspruchs 1 wird erreicht, dass der zweiten Datenverarbeitungsanlage auf sehr sichere Art und Weise die zweiten Daten zugeführt werden, wobei die zweite Datenverarbeitungsanlage mit Hilfe der zweiten Daten Authentifizierungsinformationen erzeugt, mit denen vorzugsweise automatisch ohne Eingriff einer Bedienperson eine Authentifizierungsprozedur durchführbar ist.

Ein zweiter Aspekt der Erfindung betrifft eine Anordnung zur Authentifizierung einer Datenverarbeitungsanlage. Eine erste Datenverarbeitungsanlage erzeugt erste Informationen. Die ersten Informationen werden einer zweiten Datenverarbeitungsanlage einer Bedieneinheit zugeführt. Die zweite Datenverarbeitungsanlage erzeugt mit Hilfe der ersten Informationen und einer in der zweiten Datenverarbeitungsanlage enthaltenen weiteren Information erste Daten. Die Anordnung enthält eine Datenleitung, über die erste Daten von der ersten Datenverarbeitungsanlage zur zweiten Datenverarbeitungsanlage übertragbar sind. Die erste Datenverarbeitungsanlage erzeugt abhängig von den ersten Daten zweite Daten. Die zweiten Daten sind über die Datenleitung von der ersten Datenverarbeitungsanlage zur zweiten Datenverarbeitungsanlage übertragbar. Die zweite Datenverarbeitungsanlage erzeugt mit Hilfe der zweiten Daten

Authentifizierungsinformationen zur Authentifizierung der zweiten Datenverarbeitungsanlage.

Durch diese erfindungsgemäße Anordnung wird erreicht, dass das Erzeugen und Übertragen der zweiten Daten zum Erzeugen der Authentifizierungsinformationen durch die zweite Datenverarbeitungsanlage einfach und ohne aufwendige Benutzereingriffe durchführbar ist. Ferner ist, insbesondere dadurch, dass die zweite Datenverarbeitungsanlage mit Hilfe der zweiten Daten die Authentifizierungsinformationen erzeugt, eine Authentifizierung der zweiten Datenverarbeitungsanlage durch eine weitere Datenverarbeitungsanlage und/oder die erste Datenverarbeitungsanlage einfach möglich.

Ein dritter Aspekt der Erfindung betrifft ein Verfahren zur Authentifizierung einer Bedieneinheit eines elektrofotografischen Druck- oder Kopiersystems. In einer ersten Datenverarbeitungsanlage der Bedieneinheit werden erste Daten gespeichert. Die erste Datenverarbeitungsanlage erzeugt mit Hilfe der ersten Daten eine Authentifizierungsinformation. Mit Hilfe von Authentifizierungsdaten wird die Authentifizierungsinformation zu einer zweiten Datenverarbeitungsanlage des Druck- oder Kopiersystems übertragen. Die Authentizität der ersten Datenverarbeitungsanlage wird durch die zweite Datenverarbeitungsanlage überprüft. Mit Hilfe der Authentifizierungsdaten werden durch die zweite Datenverarbeitungsanlage Zugriffsrechte der ersten Datenverarbeitungsanlage festgelegt.

Durch dieses erfindungsgemäße Verfahren wird erreicht, dass eine Authentifizierung der Bedieneinheit und das Festlegen der Zugriffsrechte der Bedieneinheit sehr einfach möglich ist. Aufwendige Bedieneingriffe einer Bedienperson sind zur Authentifizierung der Bedieneinheit nicht erforderlich.

Ein vierter Aspekt der Erfindung betrifft eine Anordnung zum Authentifizieren einer Bedieneinheit eines elektrofotografi-

schen Druck- oder Kopiersystems. Erste Daten sind in einer ersten Datenverarbeitungsanlage der Bedieneinheit gespeichert. Die erste Datenverarbeitungsanlage erzeugt mit Hilfe der ersten Daten eine Authentifizierungsinformation. Die erste Datenverarbeitungsanlage überträgt Authentifizierungsdaten zu einer zweiten Datenverarbeitungsanlage des Druck- oder Kopiersystems, wobei die Authentifizierungsdaten die Authentifizierungsinformation enthalten. Die zweite Datenverarbeitungsanlage überprüft die Authentizität der ersten Datenverarbeitungsanlage, wobei die zweite Datenverarbeitungsanlage mit Hilfe der Authentifizierungsdaten Zugriffsrechte der ersten Datenverarbeitungsanlage festlegt. Durch diese erfindungsgemäße Anordnung wird erreicht, dass eine Authentifizierung der Bedieneinheit sehr einfach durch die Bedieneinheit des Druck- oder Kopiersystems durchgeführt wird. Eingriffe von einer Bedienperson sind für eine solche Authentifizierung nicht zwingend erforderlich. Ferner wird durch diese Anordnung erreicht, dass eine sehr sichere Authentifizierung der Bedieneinheit durchgeführt wird und Fremdzugriffe auf die Datenverarbeitungsanlage des Druck- oder Kopiersystems verhindert werden.

Zum besseren Verständnis der vorliegenden Erfindung wird im Folgenden auf die in den Zeichnungen dargestellten bevorzugten Ausführungsbeispiele Bezug genommen, die an Hand spezifischer Terminologie beschrieben sind. Es sei jedoch darauf hingewiesen, dass der Schutzumfang der Erfindung dadurch nicht eingeschränkt werden soll, da derartige Veränderungen und weitere Modifizierungen an den gezeigten Vorrichtungen und/oder dem Verfahren sowie derartige weitere Anwendungen der Erfindung, wie sie darin aufgezeigt sind, als übliches derzeitiges oder künftiges Fachwissen eines zuständigen Fachmannes angesehen werden. Die Figuren zeigen Ausführungsbeispiele der Erfindung, nämlich:

Figur 1 ein Blockschaltbild eines Systems zum Erzeugen und Übertragen eines Schlüssels zur Authentifizierung eines Service- und Wartungscomputers;

Figur 2 eine Bedienoberfläche zum Anfordern des Schlüssels bei einem Autorisierungs-Server;

Figur 3 ein Blockschaltbild zur Authentifizierung des Service- und Wartungscomputers durch einen Drucker; und

Figur 4 ein Ausgabefenster mit einer Testmeldung, die bei einer fehlerhaften Autorisierung ausgegeben wird.

In Figur 1 ist ein System 10 zum Erzeugen und Übertragen eines Schlüssels 12 dargestellt, der zur Authentifizierung eines Service- und Wartungscomputers 14 durch eine weitere nicht dargestellte Datenverarbeitungseinheit eines Druckers dient. Das System 10 enthält einen Autorisierungs-Server 16, der über eine Netzwerkverbindung 18 mit dem Service- und Wartungscomputer verbindbar ist. Das Erzeugen und Übertragen des Schlüssels 12 wird auch als Freischaltungsprozedur des Service- und Wartungscomputers 14 bezeichnet. Für diese Freischaltungsprozedur ist eine Datenverbindung, z.B. über Netzwerk 18, zwischen dem Service- und Wartungscomputer 14 und dem Autorisierungs-Server 16 erforderlich.

Der Autorisierungs-Server 16 erzeugt eine sogenannte Transaktionsnummer (TAN). Die Transaktionsnummer ist eine Ziffern- und/oder Buchstabenfolge, die eine Bedienperson am Service- und Wartungscomputer zum Durchführen der Freischaltungsprozedur eingeben muss. Die vom Autorisierungs-Server 16 erzeugte Transaktionsnummer wird der Bedienperson per Post oder per E-Mail zugesendet. Die Bedienperson ist vorzugsweise ein Servicetechniker des Druckerherstellers, der einen portablen Computer, ein sogenanntes Notebook, als Service- und Wartungscomputer 14 besitzt. Im Folgenden wird der Service- und Wartungscomputer 14 des Servicetechnikers

tungscomputer 14 des Servicetechnikers als Service-Notebook bezeichnet.

Der Servicetechniker startet auf dem Service-Notebook 14 ein Programmmodul zum Durchführen der Freischaltungsprozedur, nachdem er per Post oder E-Mail die Transaktionsnummer erhalten hat. Der Servicetechniker gibt mit Hilfe einer Bedienoberfläche die Transaktionsnummer ein und startet anschließend den Freischaltungsvorgang. Das Programmmodul ermittelt ein vorbestimmtes Hardwaremerkmal, z.B. die Seriennummer des Prozessors oder eines Netzwerkadapters. Ein solches Hardwaremerkmal wird auch als "Fingerprint" des Service-Notebooks 14 bezeichnet. Über die Netzwerkverbindung 18 wird die Seriennummer und die Transaktionsnummer zum Autorisierungs-Server 16 übertragen. Der Autorisierungs-Server 16 überprüft die Gültigkeit der Transaktionsnummer und legt aufgrund der Transaktionsnummer eine Berechtigungsstufe des Service-Notebooks 14 fest, die dann bei einer späteren Verbindung des Service-Notebooks 14 mit einem Drucker die Zugriffsrechte des Service-Notebooks 14 auf die Steuereinheiten und Datenbasen des Druckers festlegt.

Der Autorisierungs-Server 16 legt weiterhin ein Gültigkeitsdatum fest, bis zu dem eine Autorisierung mit Hilfe des zu erzeugenden Schlüssels 12 durch einen Drucker möglich ist. Vorzugsweise ist auch ein Zeitraum festgelegt, in dem mit Hilfe der gesendeten Transaktionsnummer ein Service-Notebook 14 freigeschaltet werden kann. Mit Hilfe des übertragenen Hardwaremerkmals, dem Gültigkeitsdatum und der Berechtigungsstufe erzeugt der Autorisierungs-Server 16 einen sogenannten Schlüssel 12, der diese Angaben vorzugsweise in codierter Form enthält und/oder durch den zumindest eine Überprüfung dieser Angaben möglich ist. Der erzeugte Schlüssel 12 wird über das Netzwerk 18 zum Service-Notebook 14 übertragen, wobei der Schlüssel 12 in einem Speicherbereich des Service-Notebooks 14 gespeichert wird.

Mit Hilfe des Systems 10 ist somit eine Freischaltungsprozedur zum Freischalten des Service-Notebooks 14 erfolgt. Der durch diese Freischaltungsprozedur im Service-Notebook 14 gespeicherte Schlüssel 12 enthält das Hardwaremerkmal, das Verfallsdatum und die Zugriffsrechte des Service-Notebooks 14 in verschlüsselter Form.

Bei anderen Ausführungsbeispielen sind zumindest das Hardwaremerkmal, das Verfallsdatum und die Zugriffsrechte mit Hilfe des Schlüssels 12 überprüfbar. Die Transaktionsnummer kann bei weiteren Ausführungsbeispielen auch von einer separaten Institution erzeugt werden. Die Transaktionsnummer muss dann dem Servicetechniker zur Eingabe in das Service-Notebook 14 übersandt und dem Autorisierungs-Server 16 eingegeben werden. Die Netzwerkverbindung 18 ist nach Figur 1 eine Verbindung über ein Wide Area Network, wie z.B. dem Internet. Wird eine solche Verbindung über das Internet gewählt, so erfolgt die Datenübertragung vorzugsweise mit Hilfe eines gesicherten Übertragungskanals.

Alternativ kann bei anderen Ausführungsbeispielen eine Punkt-zu-Punkt-Verbindung, z.B. mit Hilfe von Modems, über ein öffentliches Telefonnetz übertragen werden. Um die Übertragungssicherheit zu erhöhen, können zur Datenübertragung weiterhin bekannte Verschlüsselungsverfahren zur Datenübertragung genutzt werden. Mit Hilfe des Systems 10 ist es weiterhin möglich, dass ein Servicetechniker das Service-Notebook 14 von einem beliebigen, mit dem Netzwerk 18 verbindbaren Ort aus freischalten kann. So ist es z.B. auch möglich, das Service-Notebook 14 von einem Telefonanschluss eines Kunden aus oder von einem beliebigen anderen Telefonanschluss aus freizuschalten.

Ist die Gültigkeitsdauer des Schlüssels 12 abgelaufen, so ist eine wiederholte Freischaltung des Service-Notebooks 14 erforderlich. Zum wiederholten Freischalten wird dieselbe Freischaltungsprozedur nochmals durchgeführt, wie bereits zuvor

für die erste Freischaltung des Service-Notebooks 14 beschrieben.

Für unterschiedliche Service-Notebooks mit gleicher Berechtigungsstufe werden durch den Autorisierungs-Server 16 unterschiedliche Schlüssel 12 erzeugt und zugewiesen. Aus diesen unterschiedlichen Schlüsseln 12 ist jedoch jeweils eindeutig die Berechtigungsstufe und der Gültigkeitszeitraum ermittelbar, ohne dass der Schlüssel 12 selbst einer Datenverarbeitungsanlage des Druckers bekannt sein muss, die die Authentizität des Service-Notebooks 14 überprüft. Dadurch wird erreicht, dass es nicht erforderlich ist, allen Druckern mitzuteilen, welche Service-Notebooks 14 der Servicetechniker und welche weiteren Bedieneinheiten eine Berechtigung zum Zugriff auf die Datenbasis und/oder die Steuereinheiten des jeweiligen Druckers haben. Ein solches Service-Notebook 14 wird als Bedieneinheit mit einem Drucker lokal oder über eine Netzwerkverbindung 18 verbunden, wobei mit Hilfe des Service-Notebooks 14 sowohl Einstellwerte des Druckers ausgelesen als auch geänderte Einstellwerte zum Drucker übertragen werden können, der Drucker mit Hilfe des Service-Notebooks 14 bedient werden kann und eine Diagnose des Druckers oder von Baugruppen des Druckers mit Hilfe des Service-Notebooks 14 durchgeführt wird.

Durch die Druckersoftware bzw. durch die Firmware des Druckers ist für jeden einzelnen Parameter festgelegt, bis zu welcher Berechtigungsstufe ein Lese- und/oder Schreibzugriff auf diesen Einstellparameter gestattet ist. Vorzugsweise werden die Schreibzugriffe auf Einstellparameter nur Benutzern mit einer hohen Berechtigungsstufe gestattet.

In Figur 2 ist eine Bedienoberfläche 20 zum Freischalten des Service-Notebooks 14 dargestellt. Die Bedienoberfläche 20 wird mit dem von dem Servicetechniker auf dem Service-Notebook 14 gestarteten Programmmodul zum Freischalten des Service-Notebooks 14 erzeugt und auf einer Anzeigeeinheit des

Service-Notebooks 14 ausgegeben. Mit Hilfe dieser Bedienoberfläche 20 kann die Bedienperson die Art der Verbindung zum Autorisierungs-Server 16 auswählen. In einem Ein- und Ausgabefeld 22 kann die Bedienperson die Netzwerkadresse oder die Internetadresse des Autorisierungs-Servers 16 auswählen oder eintragen, wenn das Service-Notebook 14 über eine Netzwerkverbindung des World Wide Web des Internets mit dem Autorisierungs-Server 16 verbunden ist. Mit Hilfe eines Auswahlfeldes 24 kann die Bedienperson alternativ eine Punkt-zu-Punkt-Verbindung des Service-Notebooks 14 mit dem Autorisierungs-Server 16 einstellen, wenn das Service-Notebook 14 und der Autorisierungs-Server 16 z.B. über Modems mit Hilfe eines Telefonnetzes verbindbar sind. Für eine solche Punkt-zu-Punkt-Verbindung kann die Bedienperson im Eingabeabschnitt 26 die erforderlichen Daten zum Verbindungsaufbau der Punkt-zu-Punkt-Verbindung eingeben. Diese Daten betreffen insbesondere einen Loginnamen und ein Passwort zum Aufbau der Verbindung und eine Telefonnummer, über die der Autorisierungs-Server über das Telefonnetz erreichbar ist. Ferner ist ein zu nutzendes Protokoll auswählbar.

Der Abschnitt 26 enthält weiterhin ein Ausgabefeld, in dem der Verbindungsstatus angezeigt wird. Mit Hilfe einer grafischen Funktionstaste 28 kann eine Verbindung über das Telefonnetz hergestellt werden. Mit Hilfe der grafischen Funktionstaste 30 kann eine bestehende Verbindung unterbrochen werden, wobei mit Hilfe der grafischen Funktionstaste 32 sowohl der Verbindungsaufbau als auch der Verbindungsabbau unterbrochen werden kann. In einem Eingabefeld 34 ist die übermittelte Transaktionsnummer (TAN) einzugeben. Nach der Eingabe der Transaktionsnummer kann die Bedienperson mit Hilfe der grafischen Funktionstaste 36 den Registrierungsvorgang beim Autorisierungs-Server 16 starten, wobei das Programmmodul sowohl die Transaktionsnummer als auch die Nummer des Prozessors des Service-Notebooks 14 zum Autorisierungs-Server 16 überträgt. Das Programmmodul enthält spezielle Programmelemente zum Ermitteln der Seriennummern

des Prozessors.

Wie bereits in Zusammenhang mit Figur 1 beschrieben, ermittelt der Autorisierungs-Server 16 mit Hilfe der Seriennummer des Prozessors und weiteren Informationen einen Schlüssel 12, nachdem er die Gültigkeit der Transaktionsnummer überprüft hat. Nach dem Erzeugen des Schlüssels 12 wird dieser zum Service-Notebook 14 übertragen. Der Schlüssel 12 wird in einem dafür vorgesehenen Speicherbereich des Service-Notebooks 14 gespeichert. Nachdem der Schlüssel 12 erfolgreich zum Service-Notebook 14 übertragen worden ist, wird die grafische Funktionstaste 38 aktiviert dargestellt, dass das Service-Notebook 14 erfolgreich freigeschaltet worden ist. Durch Aktivieren der grafischen Funktionstaste 38 wird der Freischaltungsvorgang abgeschlossen und die Abarbeitung des Programmmoduls zur Freischaltung beendet.

In Figur 3 ist ein Blockschaltbild zur Authentifizierung des Service-Notebooks 14 durch einen Drucker 40 dargestellt. Das Service-Notebook 14 ist über eine Netzwerkverbindung 42 mit dem Drucker 40 verbunden. Wie bereits in Zusammenhang mit den Figuren 1 und 2 erläutert, ist ein Schlüssel 12 im Service-Notebook 14 gespeichert, wobei der Schlüssel 12 Informationen über die Seriennummer des Prozessors, die Gültigkeitsdauer des Schlüssels 12 und die Zugriffsrechte des Service-Notebooks 14 enthält. Vorzugsweise sind diese Informationen codiert im Schlüssel 12 enthalten. Alternativ sind mit Hilfe des Schlüssels 12 diese Informationen zumindest überprüfbar.

Bevor das Service-Notebook 14 Zugriff auf Einstellparameter und Diagnosefunktionen des Druckers 40 erhält, führt der Drucker 40 eine Autorisierung des Service-Notebooks 14 durch. Dazu wird durch ein Programmmodul des Druckers über das Netzwerk 42 das Vorhandensein des Schlüssels 12 auf dem Service-Notebook 14 und die Berechtigungsstufe des Service-Notebooks 14 ermittelt. Vorzugsweise erfolgt die Autorisierung durch den Drucker 40 mit Hilfe eines Challenge- und Response-

Verfahrens. Dabei überträgt der Drucker 40 eine Zufallszahl zum Service-Notebook 14. Das Service-Notebook 14 führt mit der Zufallszahl abhängig vom Schlüssel 12 eine nicht umkehrbare mathematische Rechenoperation aus. Das Ergebnis dieser Rechenoperation wird über die Netzwerkverbindung 42 zum Drucker 40 übertragen. Der Drucker 40 überprüft das Rechenergebnis, indem er eine mathematischen Rechenoperation ausführt, die ebenfalls zu demselben Ergebnis führt. Stimmen die beiden Rechenergebnisse überein, so ist die Authentifizierung des Service-Notebooks 14 durch den Drucker 40 erfolgt.

Wie bereits erwähnt, ist für jeden Einstellparameter des Druckers 40 im Drucker 40 festgelegt, ob Nutzer mit einer vorbestimmten Berechtigungsstufe Lese- und/oder Schreibzugriffe auf den Wert des Einstellparameters haben. Ein solcher Nutzer ist z.B. das Service-Notebook 14. Nach erfolgter Authentifizierung des Service-Notebooks 14 überträgt der Drucker 40 Daten zum Erzeugen einer grafischen Benutzeroberfläche zum Bedienen, zur Konfiguration und zur Wartung des Druckers 40 zum Service-Notbook 14. Die übertragenen Daten werden mit Hilfe eines Browser-Programmoduls durch das Service-Notebook verarbetet. Die grafische Benutzeroberfläche enthält vorzugsweise Bedienoberflächen, wobei anzuzeigende Bedienoberflächen insbesondere mit Hilfe von Menüeinträgen auswählbar sind.

Die grafische Benutzeroberfläche und die Bedienoberflächen sind vorzugsweise so ausgeführt, dass sie durch den Drucker 40 automatisch an die Berechtigungsstufe des Service-Notebooks 14 angepasst wird. Ist das Service-Notebook 14 aufgrund der zugewiesenen Berechtigungsstufe nicht befugt, Lese- und/oder Schreibzugriffe auf den Einstellwert eines Einstellparameters durchzuführen, so wird dieser Einstellwert nicht bzw. nur deaktiviert dargestellt. Hat das Service-Notebook 14 nicht die Berechtigung, eine bestimmte Diagnosefunktion auszuführen, so wird diese Diagnosefunktion nicht mit über die Bedienoberfläche und/oder über Menüeinträge der

Bedienoberfläche angeboten, d.h. nicht angezeigt. Somit ist das Bedienen der Bedienoberfläche bei niedrigen Berechtigungsstufen einfacher und übersichtlicher.

Mit Hilfe einer solchen Autorisierungsprozedur, wie sie in Zusammenhang mit den Figuren 1 bis 3 beschrieben worden ist, ist es einfach möglich, versehentliche oder vorsätzliche Manipulationen und Falscheinstellungen von Einstellparametern des Drucksystems zu verhindern. Der Zugriff des Service-Notebooks 14 auf den Drucker ist dabei sowohl über eine direkte Datenleitung vor Ort als auch über eine Netzwerkverbindung, z.B. über das Internet oder ein Telefonnetz, von einem entfernten Ort aus möglich. Somit ist eine Fernwartung, Bedienung und Ferndiagnose sehr einfach möglich.

Wird die Benutzeroberfläche zum Bedienen, zur Konfiguration und zur Diagnose des Druckers 40 vom Drucker 40 über das Netzwerk 42 zum Service-Notebook 14 übertragen und auf diesem mit Hilfe eines Anzeigeprogrammmoduls, z.B. mit Hilfe eines Browsers angezeigt, so benötigt das Service-Notebook 14 lediglich Software zum Anfordern und Verwalten des Schlüssels 12, die zusätzlich zu der Standardsoftware des Service-Notebooks 14 in einem Speicherbereich des Service-Notebooks 14 gespeichert und von diesem abgearbeitet werden muss. Die Standardsoftware des Service-Notebooks 14 umfasst zumindest ein Betriebssystem und ein Browserprogrammmodul.

Vorzugsweise enthält das Browserprogrammmodul eine Java-Runtime-Programmumgebung, eine sogenannte Java-Runtime-Environment. Mit Hilfe dieser Java-Runtime-Environment ist das Abarbeiten von Java-Programmelementen, sogenannten Java-Applets sehr einfach möglich. Mit Hilfe der Java-Applets können umfangreiche Bedien-, Diagnose- und Konfigurationsfunktionen sowie eine grafische Benutzeroberfläche erzeugt werden, die über das Browserprogrammmodul ausgegeben werden. Ein Übertragen und Überprüfen von Passwörtern ist nicht erforderlich. Insbesondere beinhaltet ein solches Passwort die

Gefahr, dass z.B. bei einer Wochenend- oder Urlaubsvertretung des Servicetechnikers oder einer Bedienperson das Passwort an einen anderen Servicetechniker oder an eine andere Bedienperson weitergegeben wird. Oft werden diese Passwörter auch notiert und können so zu nicht berechtigten Personen gelangen.

Mit Hilfe der erfindungsgemäßen Authentifizierung des Service-Notebooks 14 enthält das Service-Notebook 14 alle zur Authentifizierung des Service-Notebooks 14 erforderlichen Daten. Bei einer Urlaubs- oder Wochenendvertretung wird einfach einem anderen Servicetechniker oder einer anderen Bedienperson das Service-Notebook 14 übergeben. Der vertretende Servicetechniker oder die vertretende Bedienperson erhält keinerlei Informationen, mit denen es möglich ist, nach Rückgabe des Service-Notebooks 14 mit einem anderen Service-Notebook oder einer anderen Datenverarbeitungsanlage Zugriff auf den Drucker 40 zu erhalten.

In Figur 4 ist ein Ausgabefenster mit einer Textmeldung dargestellt, das auf dem Service-Notebook 14 bei nicht erfolgter Freischaltung und bei abgelaufener Freischaltung ausgegeben wird. Mit Hilfe dieser Textmeldung wird der Servicetechniker darüber informiert, dass das Service-Notebook 14 nicht freigeschaltet ist und er keinen Zugriff auf Servicewerkzeuge, Diagnosewerkzeuge und Dokumentationen hat. Mit Hilfe der grafischen Funktionstaste 44 kann die Bedienperson das Programmmodul zur Freischaltung des Service-Notebooks 14 starten, wodurch die in Figur 2 dargestellte Bedienoberfläche ausgegeben wird. Jedoch ist eine solche Freischaltung, wie in Zusammenhang mit Figur 2 bereits erläutert, nur möglich, wenn die Bedienperson eine gültige Transaktionsnummer hat. Durch Aktivieren der grafischen Funktionstaste 46 wird das Programmmodul zum Freischalten nicht gestartet und dem Servicetechniker stehen beim Service-Notebook 14 die eine Berechtigungsstufe erfordernden Service- und Diagnosewerkzeuge sowie eine Servicedokumentation nicht zur Verfügung.

Alternativ zur Seriennummer des Prozessors kann auch eine sogenannte MAC-Adresse der im Service-Notebook 14 enthaltenen Netzwerkkarte als Hardwaremerkmal genutzt werden. Die MAC-Adresse wird auch als Ethernet-Adresse bezeichnet. Die MAC-Adresse ist eine weltweit eindeutige Kennung eines Netzwerkadapters. Sie wird in Schicht 2 des OSI-Modells zur Adressierung genutzt. Die MAC-Adresse ist in einem ROM-Speicher des Netzwerkadapters gespeichert und nicht mit Hilfe von Programmmodulen des Service-Notebooks 14 änderbar. Die MAC-Adresse ist sechs Byte lang, in denen verschlüsselt der Hersteller und die Seriennummer des jeweiligen Netzwerkadapters enthalten ist. Die MAC-Adresse ist mit bekannten Programmmodulen auslesbar. Die MAC-Adresse dient somit zur eindeutigen Identifizierung des Service-Notebooks 14.

Weiterhin ist es vorteilhaft, mehrere Benutzergruppen vorzusehen, denen jeweils eine Berechtigungsstufe zugeordnet ist. Mit einer solchen Authentifizierung können auch Kundendaten, wie z.B. Overlays, Zeichensätze und andere Ressourcen, gegen unberechtigtes Auslesen oder Ändern geschützt werden. Dabei kann auch eine Autorisierung von anderen internen und externen Bedieneinheiten des Druckers durchgeführt werden, bevor diese Bedieneinheiten Zugriff auf die Einstellparameter und Bedienfunktionen des Druckers erhalten. Dadurch wird auch eine unberechtigte Bedienung des Druckers 40, die z.B. über ein Netzwerk erfolgen kann, an dem der Drucker 40 angeschlossen ist, verhindert werden. Vorzugsweise wird dabei auch ein Verfahren zur Kryptografie genutzt, mit dem Informationen verschlüsselt und anschließend entschlüsselt werden, insbesondere ein asymmetrisches oder ein symmetrisches Verschlüsselungsverfahren. Weiterhin kann der Schlüssel 12 einen Legitimationscode enthalten. Der Schlüssel 12 ist vorzugsweise ein Public-Key oder ein Private-Key. Alternativ kann anstatt des Schlüssels 12 auch eine Signatur genutzt werden.

Obgleich in den Zeichnungen und der vorhergehenden Beschreibung bevorzugte Ausführungsbeispiele aufgezeigt und detailliert beschrieben sind, sollte dies als rein beispielhaft und die Erfindung nicht einschränkend angesehen werden. Es wird darauf hingewiesen, dass nur die bevorzugten Ausführungsbeispiele dargestellt und beschrieben sind und sämtliche Veränderungen und Modifizierungen, die derzeit und künftig im Schutzumfang der Erfindung liegen, geschützt werden sollen.

Bezugszeichenliste

10	System
12	Schlüssel
14	Service-Notebook
16	Autorisierungs-Server
18, 42	Netzwerk/Netzwerkverbindung
20	Bedienoberfläche
22	Ein- und Ausgabefeld
24	Auswahlfeld
26	Abschnitt zur Ein- und Ausgabe
28, 30, 32, 36, 38	grafische Funktionstasten
34	Eingabefeld
40	Drucker
44, 46	grafische Funktionstasten

Patentansprüche

1. Verfahren zur Authentifizierung einer Datenverarbeitungsanlage,

bei dem mit Hilfe einer ersten Datenverarbeitungsanlage (16) eine erste Information erzeugt wird, die einer zweiten Datenverarbeitungsanlage (14) einer Bedieneinheit zugeführt wird,

erste Daten von der zweiten Datenverarbeitungsanlage (14) zur ersten Datenverarbeitungsanlage (16) über eine Datenleitung übertragen werden, wobei die ersten Daten von der zweiten Datenverarbeitungsanlage (14) mit Hilfe der ersten Information und einer in der zweiten Datenverarbeitungsanlage (14) enthaltenen weiteren Information erzeugt werden,

mit Hilfe der ersten Datenverarbeitungsanlage (16) abhängig von den ersten Daten zweite Daten erzeugt werden, die von der ersten Datenverarbeitungsanlage (16) zur zweiten Datenverarbeitungsanlage (14) über die Datenleitung übertragen werden,

und bei dem durch die zweite Datenverarbeitungsanlage (14) mit Hilfe der zweiten Daten Authentifizierungsinformationen zur Authentifizierung der zweiten Datenverarbeitungsanlage (14) erzeugt werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die weiteren Informationen ein Hardwaremerkmal der zweiten Datenverarbeitungsanlage (14) enthalten.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass mit Hilfe der zweiten Daten überprüft wird, ob die zweite

Datenverarbeitungsanlage (14) das Hardwaremerkmal enthält.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten ein Verfallsdatum und Informationen enthalten, durch die Zugriffsrechte der zweiten Datenverarbeitungsanlage (14) festgelegt werden.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Zugriffsrechte mit Hilfe einer Berechtigungsstufe zugewiesen werden.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten verschlüsselt übertragen werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Datenleitung eine Netzwerkverbindung, insbesondere eine gesicherte Internetverbindung ist.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Datenverbindung eine Punkt-zu-Punkt-Verbindung ist.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten einen Schlüssel (12) enthalten.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Authentizität der zweiten Datenverarbeitungsanlage (14) von einer dritten Datenverarbeitungsanlage (40) überprüft wird, die in einem elektrofotografischen Druck- oder Kopiersystem enthalten ist.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Informationen eine Transaktionsnummer enthalten.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die ersten Informationen per E-Mail oder per Post versendet werden.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass die der ersten Datenverarbeitungsanlage (16) zugeführten ersten Informationen über eine Eingabeeinheit der ersten Datenverarbeitungsanlage (16) eingegeben werden.

14. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweite Datenverarbeitungsanlage (14) eine Bedieneinheit, insbesondere zur Konfiguration, Wartung und Bedienung, eines elektrofotografischen Druck- oder Kopiersystems ist, wobei eine dritte Datenverarbeitungsanlage (40) des Druck- oder Kopiersystems die Authentizität der zweiten Datenverarbeitungsanlage (14) überprüft.

15. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass als Hardwaremerkmal der zweiten Datenverarbeitungsanlage (14) eine vom Benutzer nicht änderbare Hardwareinformation der zweiten Datenverarbeitungsanlage (14) genutzt wird, insbesondere eine Seriennummer einer CPU oder eines Prozessors.

16. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten mit Hilfe einer Authentifizierungsprozedur verarbeitet werden, die dritte Informationen erzeugt, wobei die dritten Informationen insbesondere ein Verfallsdatum und Zugriffsrechte der zweiten Datenverarbeitungsanlage (14) enthalten.

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass die Authentifizierungsprozedur bei der Verarbeitung von mehreren zweiten Daten unterschiedlicher zweiter Datenverarbeitungsanlagen (14) dieselben dritten Daten erzeugt.

18. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Überprüfung der Authentizität der zweiten Datenverarbeitungsanlage (14) mit Hilfe einer Challenge-/Response-Prozedur erfolgt.

19. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten ein signiertes Zertifikat enthalten.

20. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweiten Daten einen Schlüssel enthalten, und dass die Authentifizierungsinformationen einen Authentifizierungscode enthalten, der mit Hilfe des Schlüssels (12) erzeugt wird.

21. Anordnung zum Erzeugen von Authentifizierungsinformationen,

bei der eine erste Datenverarbeitungsanlage (16) eine erste Information erzeugt, wobei die erste Information einer zweiten Datenverarbeitungsanlage (14) einer Bedieneinheit zugeführt wird,

die zweite Datenverarbeitungsanlage (14) mit Hilfe der ersten Information und einer in der zweiten Datenverarbeitungsanlage (14) enthaltenen weiteren Information erste Daten erzeugt,

eine Datenleitung vorgesehen ist, über die erste Daten von der ersten Datenverarbeitungsanlage (16) zur zweiten Datenverarbeitungsanlage (14) übertragbar sind,

die zweite Datenverarbeitungsanlage (14) abhängig von den ersten Daten zweite Daten erzeugt,

die zweiten Daten über die Datenleitung von der zweiten Datenverarbeitungsanlage (14) zur ersten Datenverarbeitungsanlage (16) übertragbar sind,

und bei der die zweite Datenverarbeitungsanlage (14) mit Hilfe der zweiten Daten Authentifizierungsinformationen zur Authentifizierung der zweiten Datenverarbeitungsanlage (40) erzeugt.

22. Verfahren zur Authentifizierung einer Bedieneinheit eines elektrofotografischen Druck- oder Kopiersystems,

bei dem in einer ersten Datenverarbeitungsanlage (14) der Bedieneinheit erste Daten gespeichert werden,

die erste Datenverarbeitungsanlage (14) mit Hilfe der ersten Daten eine Authentifizierungsinformation erzeugt, die mit Hilfe von Authentifizierungsdaten zu einer zweiten Datenverarbeitungsanlage (40) des Druck- oder Kopiersystems übertragen werden,

die Authentizität der ersten Datenverarbeitungsanlage (14) durch die zweite Datenverarbeitungsanlage (40) überprüft wird,

und bei dem mit Hilfe der Authentifizierungsdaten durch die zweite Datenverarbeitungsanlage (40) Zugriffsrechte der ersten Datenverarbeitungsanlage (14) festgelegt werden.

23. Verfahren nach Anspruch 22, dadurch gekennzeichnet, dass die ersten Daten einen Schlüssel (12) und/oder eine Signatur enthalten.

24. Verfahren nach Anspruch 23, dadurch gekennzeichnet, dass der Schlüssel (12) ein Public-Key und/oder ein Private-Key ist.

25. Verfahren nach einem der Ansprüche 22 bis 24, dadurch gekennzeichnet, dass die Daten zwischen der ersten Datenverarbeitungsanlage (14) und der zweiten Datenverarbeitungsanlage (40) mit Hilfe einer Netzwerkverbindung übertragen werden, wobei die erste Datenverarbeitungsanlage (16) zur Fernbedienung, Fernwartung und/oder Ferndiagnose des Druck- oder Kopiersystems dient und zumindest Zugriff auf Steuereinheiten des Druck- oder Kopiersystems nach dem Überprüfen der Authentizität hat.

26. Anordnung zum Authentifizieren einer Bedieneinheit eines elektrofotografischen Druck- oder Kopiersystems,

bei der eine erste Datenverarbeitungsanlage (14) der Bedieneinheit erste Daten enthält,

die erste Datenverarbeitungsanlage (14) mit Hilfe der ersten Daten eine Authentifizierungsinformation erzeugt,

die erste Datenverarbeitungsanlage (14) die Authentifizierungsinformationen mit Hilfe von Authentifizierungsdaten zu einer zweiten Datenverarbeitungsanlage (40) des Druck- oder Kopiersystems überträgt,

die zweite Datenverarbeitungsanlage (40) mit Hilfe der Authentifizierungsdaten die Authentizität der ersten Datenverarbeitungsanlage (14) überprüft,

und bei der die zweite Datenverarbeitungsanlage (40) mit Hilfe der Authentifizierungsdaten Zugriffsrechte der ersten Datenverarbeitungsanlage (14) festlegt.

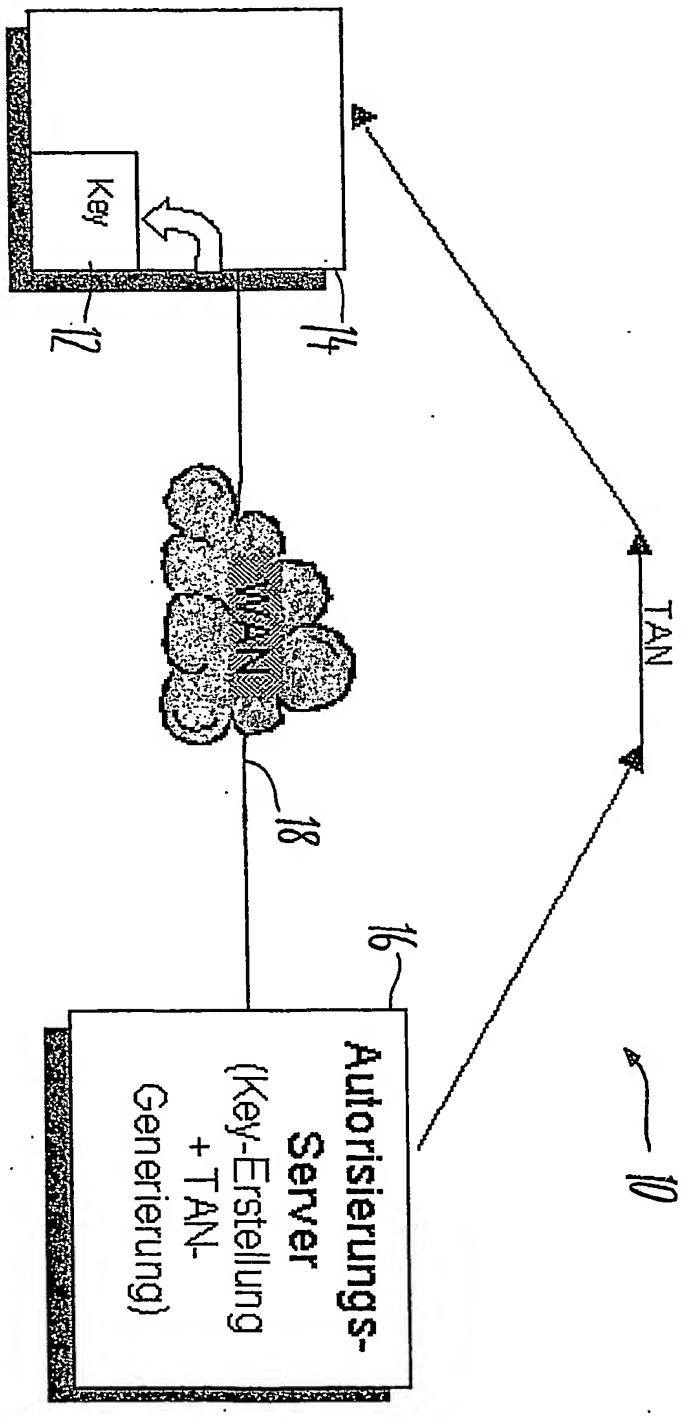
Zusammenfassung

Verfahren und Anordnung zum Authentifizieren einer Bedieneinheit sowie Übertragen einer Authentifizierungsinformation zu der Bedieneinheit

Die Erfindung betrifft ein Verfahren und eine Anordnung zum Erzeugen von Authentifizierungsinformationen. Eine erste Datenverarbeitungsanlage (16) erzeugt eine erste Information, wobei die erste Information einer zweiten Datenverarbeitungsanlage (14) einer Bedieneinheit zugeführt wird. Die zweite Datenverarbeitungsanlage (14) erzeugt mit Hilfe der ersten Informationen einer in der Datenverarbeitungsanlage (14) enthaltenen weiteren Information erste Daten. Die ersten Daten werden von der ersten Datenverarbeitungsanlage (16) zur zweiten Datenverarbeitungsanlage (14) mit Hilfe einer Datenleitung übertragen. Die erste Datenverarbeitungsanlage (16) erzeugt abhängig von den ersten Daten zweite Daten. Die zweiten Daten werden von der ersten Datenverarbeitungsanlage (16) zur zweiten Datenverarbeitungsanlage (14) übertragen. Die zweite Datenverarbeitungsanlage (14) erzeugt mit Hilfe der zweiten Daten Authentifizierungsinformationen zur Authentifizierung der zweiten Datenverarbeitungsanlage (14). Ferner betrifft die Erfindung ein Verfahren und eine Anordnung zur Authentifizierung einer Bedieneinheit eines elektrofotografischen Druck- oder Kopiersystems.

(Figur 1)

ZUSAMMENFASSUNG



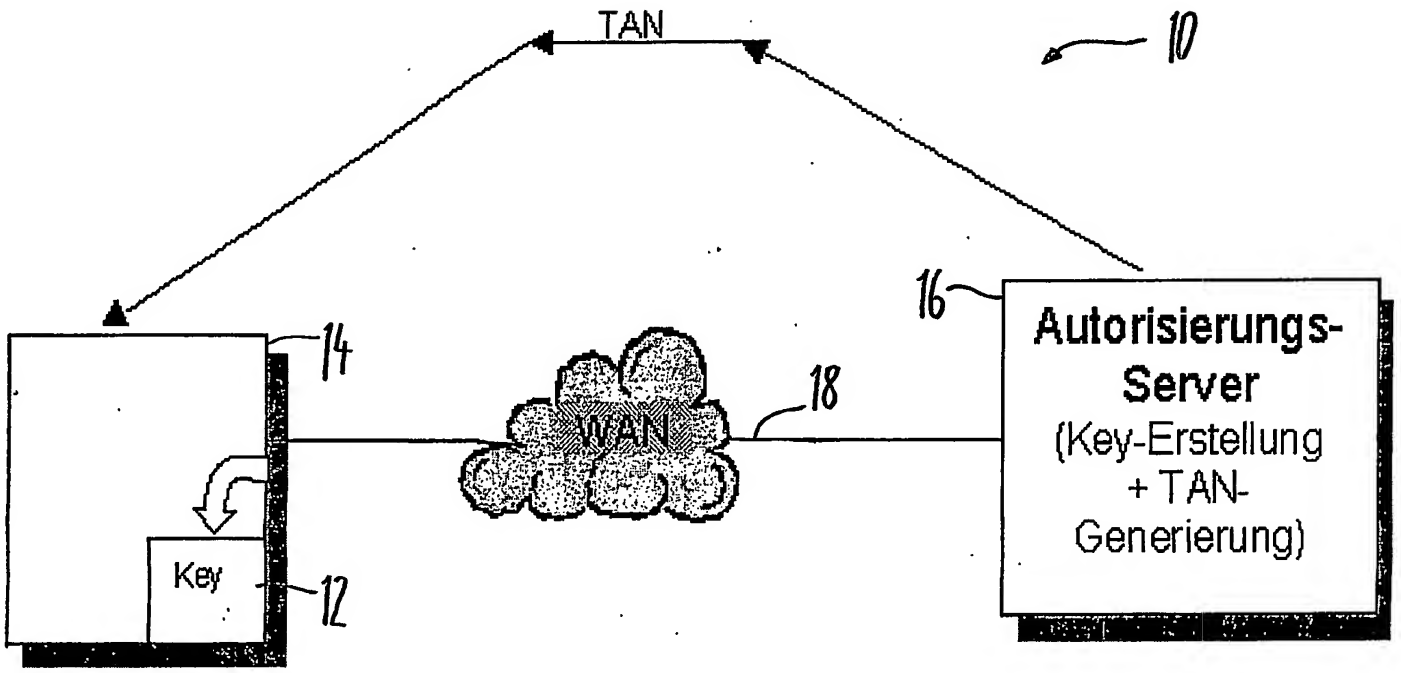

TAN
10
16
Autorisierungs-
Server
(Key-Erstellung
+ TAN-
Generierung)
14
WAN
18
Key
12

Fig. 1

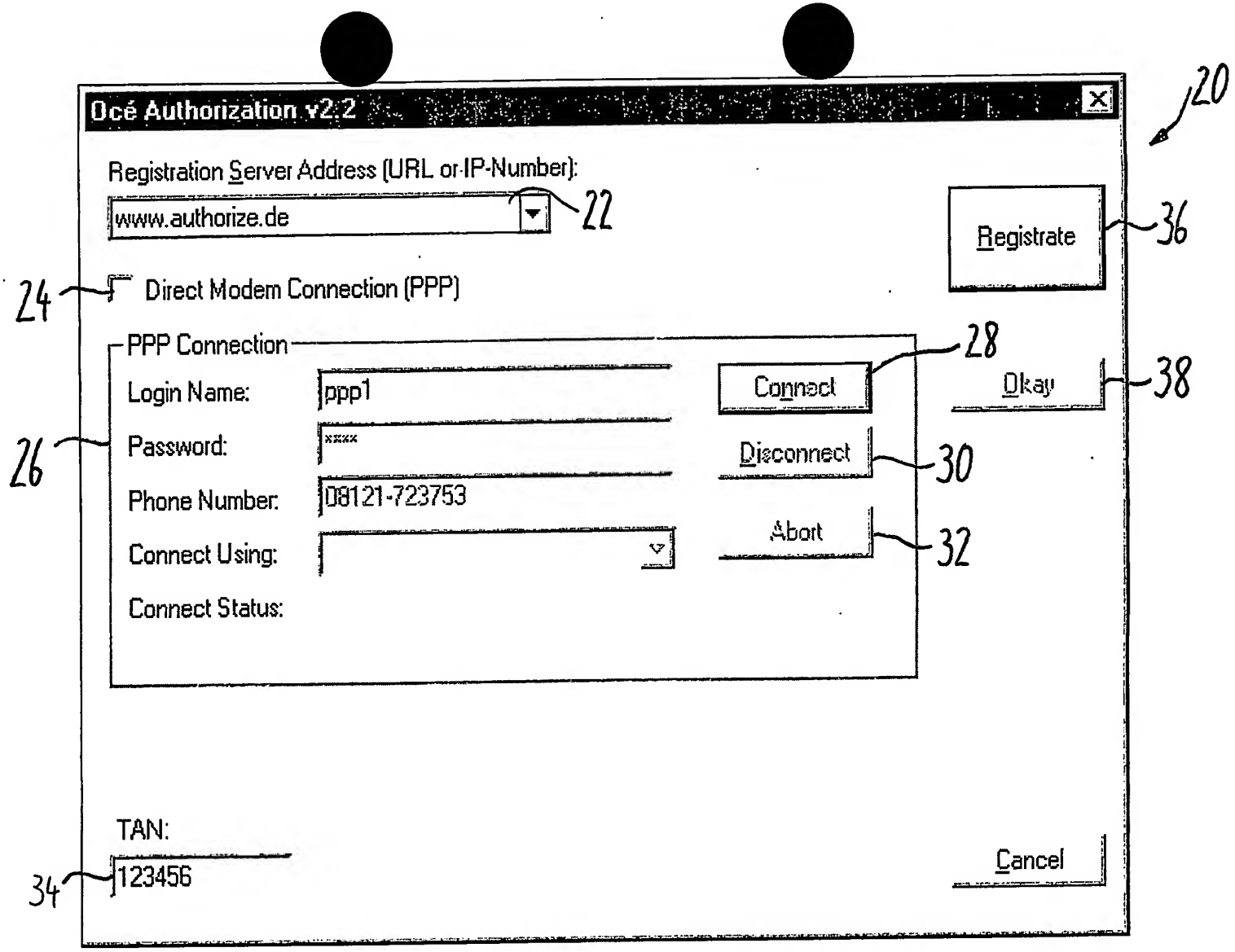

Océ Authorization v2.2
20
Registration Server Address (URL or IP-Number):
www.authorize.de
22
Registrate
36
24
Direct Modem Connection (PPP)
PPP Connection
28
Login Name:
ppp1
Connect
Okay
38
26
Password:
****
Disconnect
30
Phone Number:
08121-723753
Abort
32
Connect Using:
Connect Status:
TAN:
34
123456
Cancel

Fig. 2

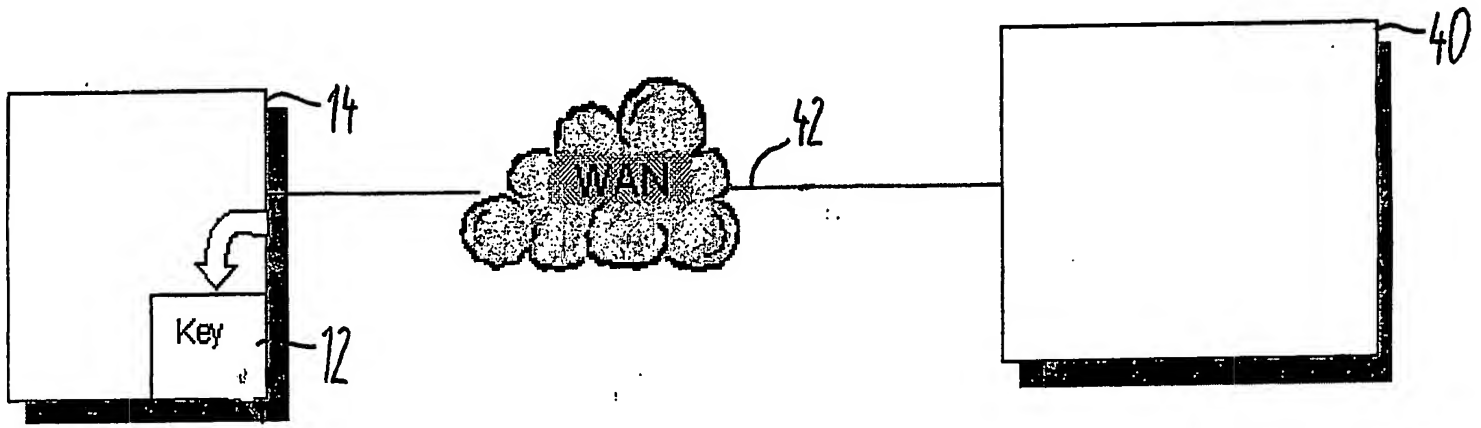


Fig. 3

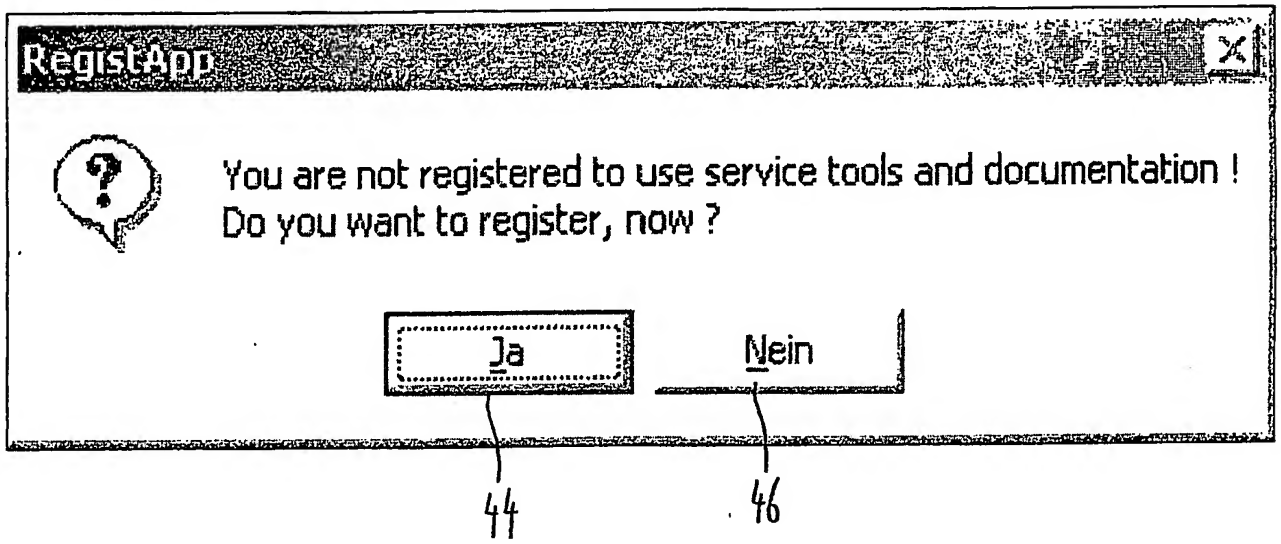

RegistApp
You are not registered to use service tools and documentation !
Do you want to register, now ?
Ja
Nein
44
46

Fig. 4